A Proposed Federal PKI Using X.509 V3 Certificates

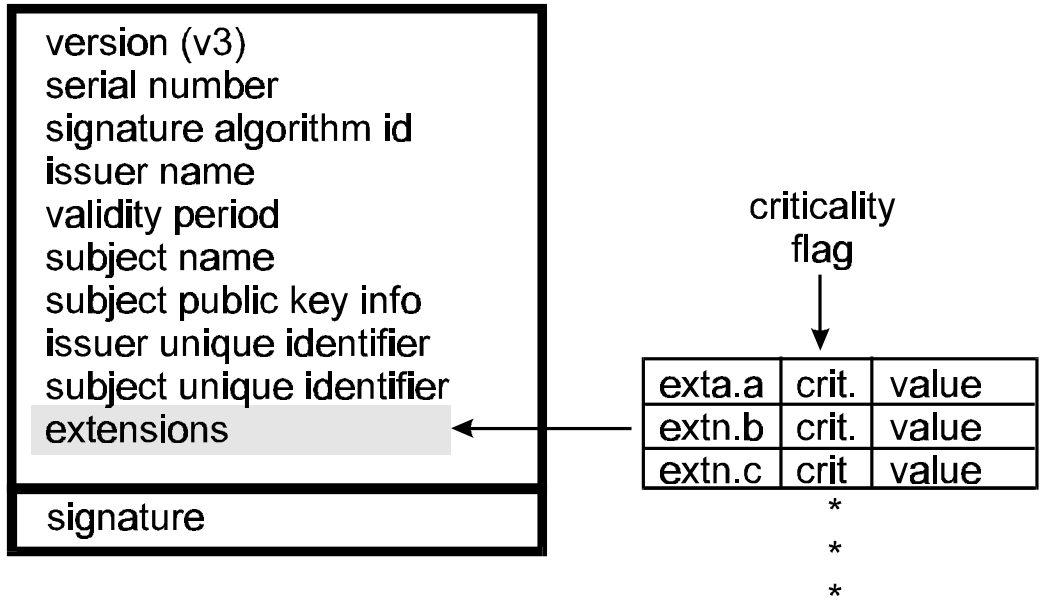
William E. Burr

Noel A. Nazario

W. Timothy Polk

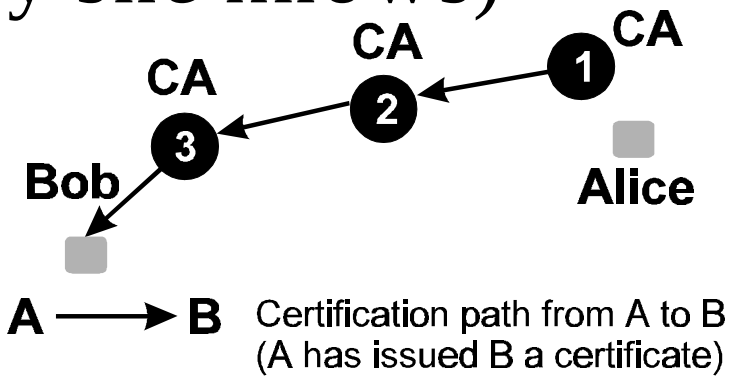
X.509 v3 Certificate

- Extensions
  - criticality flag
  - standardized extensions

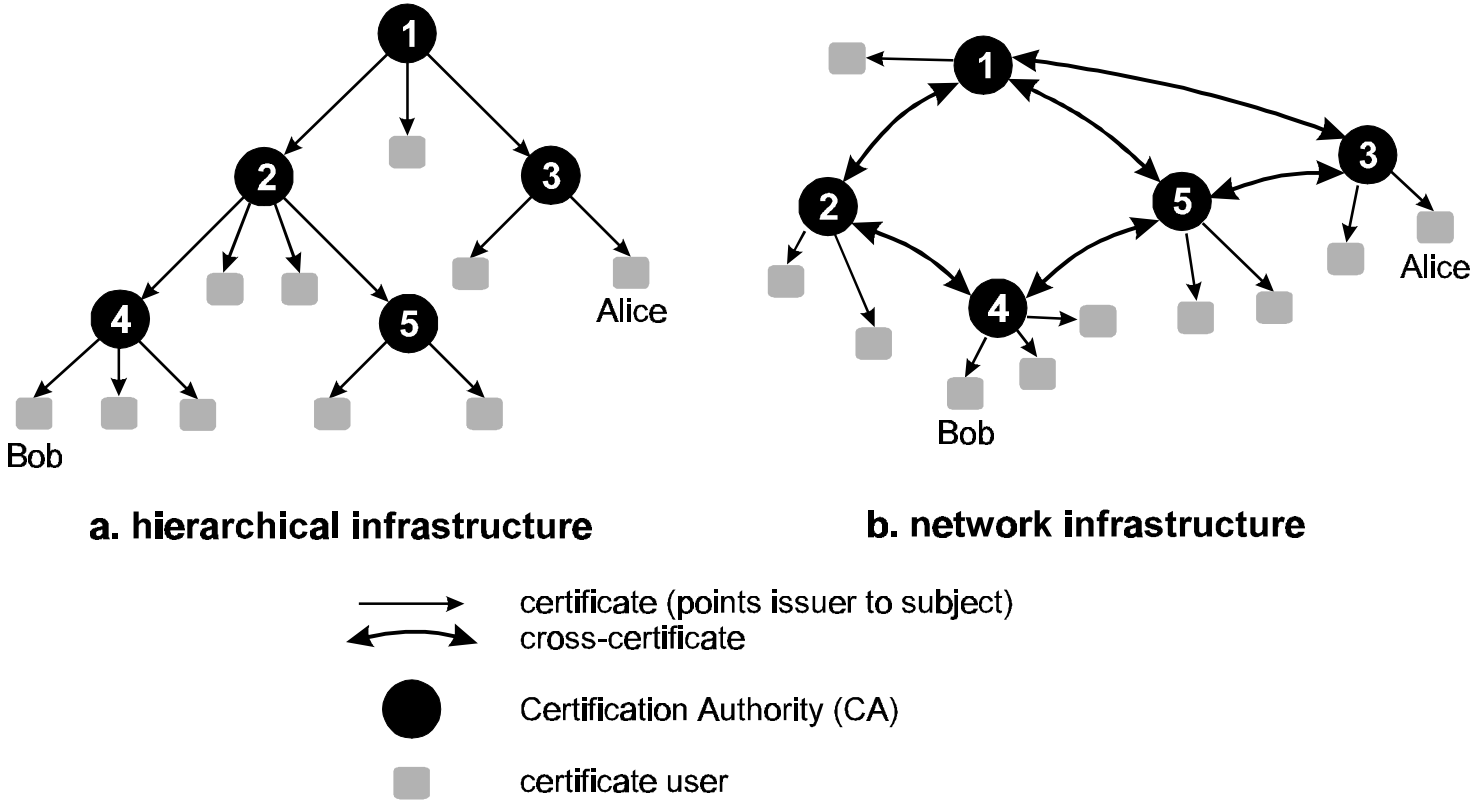


Certification Path

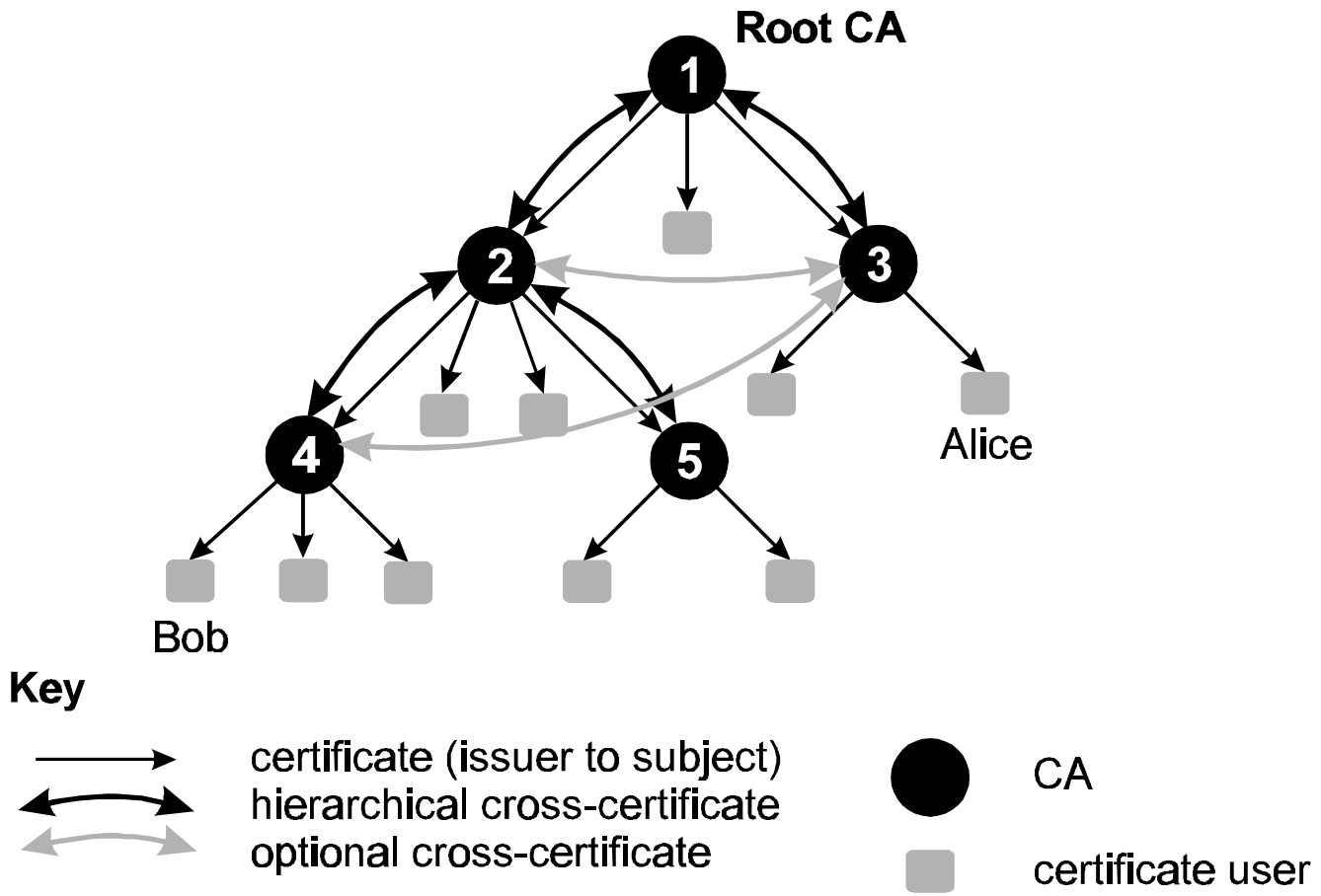
- Alice can verify Bob's certificate by verifying a chain of certificates ending in one issued by a Certification Authority (CA) she trusts (and whose public key she knows)



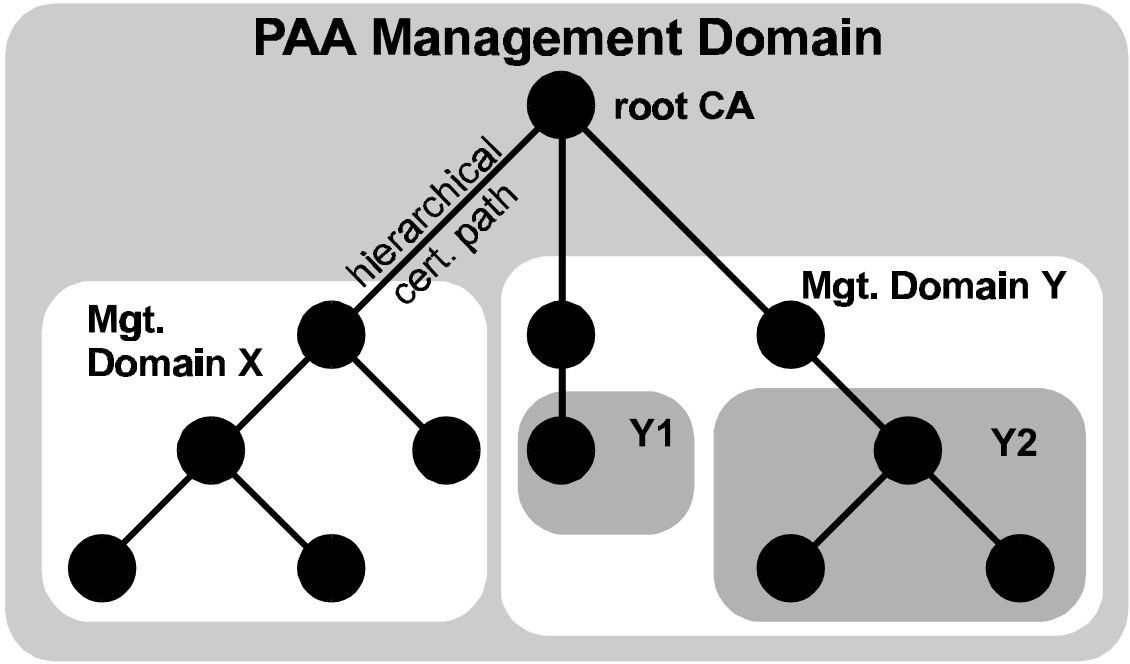
PKI: Hierarchy vs. Network



Hybrid Architecture



FPKI Management Domains



Hierarchical Management

- pathLenConstraint
  - limits length of certification path
- nameConstraint
  - limits name space a CA may issue certs. for
- certificatePolicies
  - Federal Assurance level
    - a system to give a relative level of trust

Federal Assurance Level

- OID goes in certificatePolicies extension in all Federal certificates
- Based on PAA evaluation of CA operational policy and certificate issuance policy
- States a relative trust assurance level
  - a few levels defined, such as: high, medium and low

Cross-Certificates: 3 Types

- hierarchical
  - parallels hierarchical certificates
  - uses superior to subordinate cert.
  - required
- general
- special

General Cross-Certificates

- May provide shorter cert. paths
- Allowed between any two Federal CAs
- Includes constraints at least as restrictive as those along root CA path
  - pathLenConstraint
  - nameConstraint
  - certificatePolicies
    - Federal Assurance Level (trust level indication)

Special Cross-Certificates

- Cannot be chained to other CA certificates to extend trust
  - Only between “leaf” CAs with “root certificate” pathLenConstraint of zero
  - Special cross-certificates have pathLenConstraint value set to zero
- Any other constraints are agreed between cross-certifying CAs

Conclusion

- Hybrid architecture
  - allows coherent management of FPKI
  - supports root or local CA centered trust models
- Special cross-certificates
  - allows CAs broad freedom to cross-certify
  - trust does not propagate to users of other CAs